The RUSI Journal

ISSN: 0307-1847 (Print) 1744-0378 (Online) Journal homepage: https://www.tandfonline.com/loi/rusi20

Brexit and Cyber Security

Tim Stevens & Kevin O'Brien

To cite this article: Tim Stevens & Kevin O'Brien (2019) Brexit and Cyber Security, The RUSI Journal, 164:3, 22-30, DOI: 10.1080/03071847.2019.1643256

To link to this article: https://doi.org/10.1080/03071847.2019.1643256

Published online: 25 Jul 2019.

Research Article
The RUSI Journal

Brexit and Cyber Security

Tim Stevens and Kevin O'Brien

Brexit is likely to have an effect on UK–EU cyber security cooperation. While there are ongoing reasons to be positive about the state of UK–EU cyber security, Tim Stevens and Kevin O'Brien show how Brexit will have negative impacts on cybercrime policing and cyber threat intelligence sharing, particularly in a 'no-deal' scenario, and argue that the absence of a negotiated settlement will damage the cyber security of the UK and the EU.

It is not yet clear when, or on what terms, the UK will leave the EU. By 31 October 2019, the UK must decide to ratify an exit treaty, request a further extension, cancel Brexit or opt for a no-deal departure. In the latter scenario, it will depart without a formal agreement on its future relationship with its EU security and defence partners. Deal or no deal, there will be consequences for British and European cyber security, as discussed in this article. Cyber security – the technology, processes and controls supporting the protection of computer systems, networks, devices and data from subversion, theft or damage – has not been a major topic in Brexit discussions, either diplomatically or in the public domain. Indeed, given its crucial role in furthering economic prosperity and political stability, it feels rather overlooked.

It may be that parties to the UK's withdrawal from the EU are relatively sanguine about the limited effects of Brexit on cyber security. For instance, the chief executive of the UK National Cyber Security Centre (NCSC), Ciaran Martin, has suggested that many UK–EU cyber security relationships have little or nothing to do with the EU as such. They instead rely on other bilateral and multilateral frameworks.[1] While this is true – for example, intelligence is shared with Five Eyes partners and NATO Allies – it should not mask the potentially deleterious effects of Brexit on other aspects of cyber security contingent on the EU. The UK's cyber security relationships with the EU are at least as complex as any comparable defence arrangements under the Common Security and Defence Policy: many cyber security competences fall across multiple fields of security, policing, justice and defence. Moreover, as bilateral arrangements with EU members may at some juncture be subject to the decisions of the European Court of Justice (ECJ), the relationship with the EU will have continuing relevance.

This article addresses a range of factors that should be considered when negotiating the cyber security components of a future UK–EU security treaty (or treaties) under any form of Brexit. This is particularly important in the event of a no-deal Brexit, as neither the UK nor the EU will be working from an agreed understanding of their defence, policing and security priorities and obligations – including those concerning cyber security. This article cannot provide an exhaustive analysis of the possible post-Brexit settlement of cyber security cooperation between the UK and the EU. Instead, it seeks to focus on the post-Brexit cyber security landscape more than existing EU cyber security frameworks. The first section suggests that the UK and Europe are working from positions of relative strength in cyber security, although this is not grounds for complacency. Subsequent sections address issues connected to intelligence sharing, cybercrime, and being 'outside the room' of EU cyber security decision-making. The article concludes with a call to address cyber security as a strategic priority in any future post-Brexit treaty negotiations between the UK and the EU. The conclusion is that there are reasons to be positive about future UK–EU cyber security cooperation, but this should not obscure the need for urgent and timely interventions on a range of practical and political cyber security issues.

1. Vivienne Clarke, 'Brexit "Will Not Impact" UK-EU Co-operation on Cybersecurity', *Irish Times*, 1 November 2018.

© The Author(s) Vol. 164, No. 3, April 2019 pp. 22–30

After Brexit, the UK wants to be more than just a visitor to Europol, one of the EU's key agencies coordinating action against cybercrime. *Courtesy of PA Images/Yuriko Nakao*

A Positive Baseline

In the first instance, it should be recognised that the UK is in a relatively strong position in terms of its own attitudes and commitments to cyber security. Cyber security will remain a Tier One priority for the UK, as set out in the 2015 National Security Strategy and Strategic Defence and Security Review.[2] Preparations are already underway for the fourth iteration of the National Cyber Security Strategy, following earlier versions in 2009, 2011 and 2016.[3] Government investment in cyber security has been sustained, the most recent tranche being the £1.9-billion five-year investment programme announced in 2016.[4] The founding of the NCSC has been a welcome addition to the UK cyber security landscape and allows for a greater range of proactive public–private interactions than ever.[5] The NCSC is a hub around which multiple other industry, education, standards and technical initiatives gravitate and is widely considered a potential model for other countries to emulate. The UK has also adopted new data protection and critical infrastructure regulations that will improve cyber security and consumer confidence.[6] On the commercial side, the UK has a vibrant and innovative cyber security industry worth at least £5.7 billion a year, and which works in partnership with government to deliver its strategic objectives.[7] Concerns abound, however, as to how this industry could be negatively impacted by any form of Brexit – especially a no-deal one – due to tangible evidence of lowering investments in the UK by corporations,[8] and a reduction in the number of cyber security professionals coming from the rest of the world to work in the UK.[9] This is at a time when there is already insufficient cyber security talent to meet global demand,[10] and when actual investment

2. HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom* (SDSR 2015), Cm 9161 (London: The Stationery Office, 2015).
3. Cabinet Office, 'National Cyber Security Strategy 2016-2021: Progress Report', May 2019, p. 22.
4. HM Government, 'National Cyber Security Strategy 2016-2021', November 2016.
5. National Cyber Security Centre, 'The National Cyber Security Centre', <https://www.ncsc.gov.uk/>, accessed 18 June 2019.
6. Information Commissioner's Office, 'GDPR and NIS', <https://ico.org.uk/for-organisations/the-guide-to-nis/gdpr-and-nis/>, accessed 18 June 2019.
7. RSM, 'UK Cyber Security Sectoral Analysis and Deep-Dive Review', June 2018.
8. Gavin Jackson, 'Why Investment by UK Companies Continues to Fall', *Financial Times*, 7 January 2019.
9. Joint Committee on the National Security Strategy, 'Cyber Security Skills and the UK's Critical National Infrastructure', Second Report of Session 2017-19, HL Paper 172 / HC 706, July 2018. The report notes a shortage of 15–30% of required positions in the field; a mere 10% of those positions are filled by women.
10. William Crumpler and James A Lewis, 'The Cybersecurity Workforce Gap', Center for Strategic and International Studies, January 2019. The report suggests that 82% of employers reported a shortfall in cyber security skills, while 71% believe the

DOI: 10.1080/03071847.2019.1643256

in cyber security services by British companies is, on the whole, rising year on year.[11] The overall picture is one in which UK companies are increasing their demand for cyber security skills in a severely tight labour market for those skills, a significant percentage of which are sourced from the global market, which is itself already facing a deepening cyber security skills shortage.

At the international level, the UK has also demonstrated its willingness to engage with external partners in the form of intelligence sharing, norms promotion, and diplomacy around attribution of cyber operations to foreign actors. The Attorney General's Chatham House speech of May 2018 was well-received internationally, as it set out in measured and principled fashion the UK's continuing commitment to the rule of international law in cyberspace.[12] These ambitions were demonstrated in practical terms by the UK's public attribution, in coordination with security partners, of cyber operations to Russian military intelligence in late 2018.[13] The UK's consistency in this respect suggests that it is developing a coherent approach to both theory and practice across a number of policy areas that pertain to state behaviours in cyberspace, not least in the diplomatic domain.

The UK takes seriously its relationships with its EU partners and senior British officials have expressed their confidence that Brexit will not materially affect UK–EU cyber security cooperation.[14] Institutions like the NCSC have received 'clear instruction' from the Cabinet Office to 'cooperate unconditionally on European security'.[15] Cyber security received specific attention in the Political Declaration of November 2018, identifying cooperation in cyber threat intelligence-sharing and continued partnerships with key EU cyber security institutions as strategic priorities for both parties.[16] However, it is not legally binding and will be irrelevant in the case of no deal. Other structures will continue. The April 2018 transposition into UK law of the EU Directive on Security of Network and Information Systems (NIS Directive) is a crucial aspect of both UK cyber security and EU cyber resilience strategy and will persist after Brexit, with or without a deal. The NIS Directive regulates and incentivises national cyber security capabilities and critical infrastructure cyber security.[17] In the UK, all essential sectors – such as water, energy, finance, health and transport – now have an established Competent Authority (CA), responsible for the oversight and enforcement of improved cyber security measures and reporting.[18] In the event of preventable cyber security incidents leading to serious adverse effects on essential services, the CAs are authorised to levy large fines from offending service operators. Moreover, it encourages transnational collaboration, including through the NIS Cooperation Group and the Computer Security Incident Response Teams (CSIRTs) Network.[19]

Government has reaffirmed many of these ambitions and initiatives in subsequent statements and more formally in the 2018 National Security Capability Review.[20] None of these attributes and aspirations are likely to be greatly affected by Brexit, nor are they grounds for complacency. Indeed, there are already a number of issues and concerns

talent gap causes direct and measurable damage to their organisations. The number of unfilled cyber security positions has risen by more than 50% since 2015.

11. RSM, 'UK Cyber Security Sectoral Analysis and Deep-Dive Review'.
12. Jeremy Wright, 'Cyber and International Law in the 21st Century', speech given in London, 23 May 2018, <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>, accessed 18 June 2019. For an informed reaction to this speech, see Matthew Waxman, 'U.K. Outlines Position on Cyberattacks and International Law', *Lawfare*, 23 May 2018.
13. Foreign Office, 'UK Exposes Russian Cyber Attacks', press release, 4 October 2018, <https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks>, accessed 18 June 2019.
14. Warwick Ashford, 'UK Committed to Working with EU Cyber Security Partners', *Computer Weekly*, 21 February 2019.
15. Clarke, 'Brexit "Will Not Impact" UK-EU Co-operation on Cybersecurity'.
16. 'Political Declaration Setting Out the Framework for the Future Relationship Between the European Union and the United Kingdom', 22 November 2018, ss. 110–13.
17. European Union Agency for Network and Information Security (ENISA), 'NIS Directive', <https://www.enisa.europa.eu/topics/nis-directive>, accessed 18 June 2019.
18. Department for Digital, Culture, Media and Sport, 'Security of Network and Information Systems: Guidance for Competent Authorities', April 2018.
19. Computer Security Incident Response Teams (CSIRTs) Network consists of EU member states' formally appointed national CSIRTs and CERT-EU. For more details, see ENISA, 'CSIRTs Network', <https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network>, accessed 18 June 2019.
20. HM Government, 'National Security Capability Review', March 2018, pp. 21–22.

confronting the UK's approach to cyber security irrespective of Brexit. Recent public statements by government officials over Huawei and 5G supply-chain security indicate the complex interdependencies of telecommunications policy, industrial investment and geopolitics.[21] Others have suggested that the UK government's approach to Huawei, specifically, is 'at best naive, at worst irresponsible'.[22] This may be one clear area of divergence from EU partners, as the UK, Germany, France, Italy and other leading EU countries have each yet to settle on a consistent approach on whether to allow Huawei to participate in their 5G build-outs, in the face of similar bans enacted recently in the US and Australia.[23]

As noted above, warnings continue about a cyber security skills shortage in the UK.[24] At least one parliamentary committee has called into question an apparent lack of cyber security leadership at the heart of government.[25] Worryingly, the National Audit Office's February 2019 assessment of the current National Cyber Security Programme finds that the UK government is unlikely to deliver on most of its stated strategic outcomes by 2021.[26] Some, or indeed all, of these could have an impact on the UK's future cyber security relationships with the EU. And, notwithstanding warm words to the contrary, there are other problems ahead in the way that the EU and the UK interact on cyber security issues.

Cyber Threat Intelligence

Cyber security is an inherently transnational endeavour, given the nature of the internet and other information networks which sprawl across multiple jurisdictions and regulatory boundaries. Effective cyber security is therefore contingent on the exchange of high-quality cyber threat intelligence (CTI) – and consequent remediation and mitigation actions – between key stakeholders, which include government security and intelligence agencies, cyber security firms, organisations like computer emergency response teams (CERTs), and a range of other concerned actors. CTI data is mostly derived from open sources and need not be secret in origin, although may be augmented with intelligence on pronounced cyber actors gained from covert sources as appropriate.[27] Effective use of CTI gives organisations a clear picture of the cyber threat landscape, enabling them to prevent, deter, or, at the very least, prepare for future adversarial operations. This is recognised in the Political Declaration, which identifies 'cyber-threats' as a specific reason for 'timely and voluntary' exchanges of intelligence.[28]

One of the key EU mechanisms for the sharing of CTI is CERT-EU, based in Brussels. Its core mission is to help secure EU institutions' information and communications systems, including through sharing CTI with member-states' CERTs and specialist information security firms.[29] It is unclear what form the UK's continued interactions with CERT-EU will take in the event of Brexit, as it will not have automatic access to the data of any EU institution, CERT-EU included. Like Norway and Switzerland, neither of which is a member of the EU, the NCSC is already a member of the non-EU European Government CERTs (EGC) group and the global Forum of Incident Response and Security Teams. These organisations focus beyond the EU institutions that are within CERT-EU's purview.[30] The UK may

21. David Bond, 'Huawei Threat Uncovers Enemy Within UK Spy Agencies', *Financial Times*, 1 March 2019.
22. Charles Parton, 'China-UK Relations: Where to Draw the Border Between Influence and Interference?', *RUSI Occasional Papers* (February 2019), p. 26. See also Bob Seely, Peter Varnish and John Hemmings, 'Defending Our Data: Huawei, 5G and the Five Eyes', Henry Jackson Society, London, May 2019.
23. Julian E Barnes and Adam Satariano, 'U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist', *New York Times*, 17 March 2019; Jeanne Whalen and Griff White, 'U.S. Blacklisting of Huawei Prompts European Firms to Follow Suit', *Washington Post*, 22 May 2019.
24. Joint Committee on the National Security Strategy, 'Cyber Security Skills and the UK's Critical National Infrastructure'.
25. Joint Committee on the National Security Strategy, 'Cyber Security of the UK's Critical National Infrastructure', Third Report of Session 2017–19, HL Paper 222 / HC 1708, November 2018, ss. 79–81.
26. National Audit Office, *Progress of the 2016–2021 National Cyber Security Programme*, HC 1988 (London: National Audit Office, 2019).
27. For an example of cyber threat intelligence production and consumption, see Bank of England, 'CBEST Intelligence-Led Testing: Understanding Cyber Threat Intelligence Operations', version 2.0, 2016.
28. 'Political Declaration Setting Out the Framework for the Future Relationship Between the European Union and the United Kingdom', s. 105.
29. CERT-EU, 'RFC 2350', 25 January 2019, <http://cert.europa.eu/static/RFC2350/RFC2350.pdf>, accessed 18 June 2019.
30. See European Government CERTs Group, 'European Government CERTs (EGC) Group', <http://www.egc-group.org/>, accessed 18 June 2019; Forum of Incident Response and Security Teams, <https://www.first.org/>, accessed 18 June 2019.

look to the EGC for greater cyber information sharing – but the EGC is an informal club of only 12 (plus CERT-EU), in contrast to the CERT-EU membership of 27. The Political Declaration affirmed each party's commitments to 'security and stability in cyberspace', the need to share intelligence products and to cooperate in efforts against cyber threats, and the desirability of continued UK involvement in CERT-EU and the EU Agency for Network and Information Security (ENISA).[31] These are admirable and necessary ambitions but have no legal effect in the absence of a negotiated settlement, nor is there any precision or clarity over how these outcomes might be achieved. All the more reason, therefore, that they should be part of any future negotiations over cyber security.

The UK will therefore become a 'third country' in most post-Brexit scenarios, unless it can negotiate an alternative status before 31 October 2019. There is a historical precedent: the 1997 Treaty of Amsterdam afforded the UK, by virtue of its then-status as an EU member, access to Schengen Area cooperative frameworks, including the Schengen Information System (SIS) security and law enforcement database maintained under the auspices of the European Commission. Unlike Norway and Switzerland, the UK cannot fall back on Schengen membership should it withdraw from the EU; Brexit therefore threatens its SIS access.[32] Similarly, if the UK wants access to CERT-EU data, particularly in a no-deal situation, it would have to negotiate that access, but from a significantly weakened negotiating position. At that point, it will be outside the EU and excluded from EU agenda-setting and decision-making processes. As such, it may be forced to accept EU priorities and stipulations that would not have arisen otherwise, including being bound, at least to a degree, by the decisions of the ECJ as a condition of 'doing business' with the EU. It is undoubtedly the case that the EU would prefer to be able to share CTI with the UK through existing frameworks because the UK is a substantial producer of CTI and a major cyber security player in its own right, but the UK cannot rely solely on its relative strengths to incentivise the creation of future information-sharing arrangements. By the government's own admission, in a no-deal scenario 'the ability to cooperate on cyber with the EU would be less certain and would depend on the continued willingness of all partners to share information, exchange best practice and work together to identify evolving threats'.[33] While true, this is not an exhaustive list of requisite foundations for cooperation, not least of which must include the existence of a treaty enabling cooperation in law, rather than on the basis of aspirations alone.

Brexit will affect some forms of CTI, but not all; it will also not affect many other strategic and operational intelligence-sharing arrangements existing alongside those covering CTI. The EU has access to formal intelligence-sharing mechanisms – in the Club de Berne voluntary intelligence-sharing forum, which includes the EU member states' intelligence agencies and the EU Intelligence and Situation Centre of the EU External Action Service – but these have often been accused of being ineffective, largely due to mistrust between national intelligence agencies.[34] The Counter Terrorism Group of EU countries and others has been a notable success, and the UK is expected to remain part of it, but it is not an EU institution.[35] In 2018, Director General of the Security Service (MI5) Andrew Parker drew attention to the need to deepen relations between British and other European intelligence agencies, presumably as an attempt to forestall concerns over Brexit.[36] Brexit will not immediately affect how the UK shares most intelligence with European partners, as it can do so through existing or new relationships (such as NATO, bilateral) with no basis in EU law or institutions. Sometimes this will have a cyber component: the recent public attribution of cyber incidents demonstrates this in action, as the UK and other countries, including in the EU, banded together in various configurations to identify the perpetrators.[37] European countries will want to maintain those relationships, as UK intelligence is highly regarded abroad. So too are its deep links with US intelligence structures, although UK intelligence chiefs have made it plain that they

31. 'Political Declaration Setting Out the Framework for the Future Relationship Between the European Union and the United Kingdom', ss. 110–13.
32. Alexander Babuta, 'No Deal, No Data? The Future of UK–EU Law Enforcement Information Sharing', RUSI Briefing Paper, February 2019.
33. HM Government, *EU Exit: Assessment of the Security Partnership*, Cm 9743 (London: The Stationery Office, 2018), p. 25.
34. Hartmut Aden, 'Information Sharing, Secrecy and Trust Among Law Enforcement and Secret Service Institutions in the European Union', *West European Politics* (Vol. 41, No. 4, June 2018), pp. 981–1002.
35. Ewen MacAskill, 'MI5 Chief: UK and EU Intelligence Sharing "Never More Important"', *The Guardian*, 13 May 2018.
36. *Ibid*.
37. See, for instance, Foreign Office, 'UK Exposes Russian Cyber Attacks'.

oppose any attempts to make intelligence-sharing a bargaining chip in EU–UK negotiations.[38]

Cybercrime

In one specific area of intelligence and security cooperation, Brexit may have serious and undesirable effects. In terms of volume, by far the biggest cyber security challenge is cybercrime and Brexit will impact the UK's policing and judicial counter-cybercrime capacities.[39] Europol, its subsidiary the European Cybercrime Centre, and Eurojust are important forums for EU–UK cybercrime cooperation. Europol's Secure Information Exchange Network Application and Europol Information System platforms have become invaluable tools for secure and rapid exchange of sensitive data for European law enforcement, including the National Crime Agency and other forces in the UK. The UK – with Germany – is the highest contributor of information to various Europol intelligence projects, including cyber security.[40] It also often leads on Europol operations and a Briton, Rob Wainwright, was director of Europol between 2009 and 2018.

In a no-deal situation, the UK will relinquish membership of these agencies and access to their intelligence platforms will be seriously disrupted, based on how EU law – in the development of which the UK played its part – operates. This would affect all institutional frameworks and structures with a basis in EU law, like Europol and Eurojust. In the case of a no deal, the UK would become overnight a 'third country' with respect to EU mechanisms and would be excluded *a priori* from information-sharing arrangements, including key policing databases.[41] UK police cannot assume continued access to EU databases on an ad hoc or de facto basis after Brexit: Article 8 of the draft Withdrawal Agreement clearly states that the UK must ensure 'it does not access a network, information system or database which it is no longer entitled to access'.[42]

Former Europol Director Wainwright acknowledged while still in post that the UK would face 'impediments' to information sharing after Brexit.[43] This is perhaps a diplomatic understatement, as it is unclear on what grounds the UK could reach an agreement on information sharing with Europol if a deal cannot be reached before the UK leaves the EU. It will not be a full member, being outside the EU, and would have to broker a third-country 'operational agreement' with Europol.[44] The UK government has indicated that no third-country precedent satisfies its ambitions.[45] It might be possible to negotiate a Denmark-style agreement, which is in the EU but not in Europol, but this would require the UK to accept the jurisdiction of the ECJ. This would be unacceptable to many pro-Brexit members of parliament, but outgoing Prime Minister Theresa May indicated her willingness to accept the remit of the ECJ in this particular instance if it means retaining some of the benefits of membership in Europol and other EU agencies.[46] It is unclear if the post-May government will adhere even to this minimal concession with respect to the jurisdiction of the ECJ over UK affairs. There still exists the possibility for a 'bespoke' arrangement with Europol, but all likely scenarios see the UK relegated from the core to the periphery of Europol operations and leadership.[47]

38. Ewen MacAskill, 'Using Security as Brexit Bargaining Chip is Reckless and Lacks Credibility', *The Guardian*, 30 March 2017.
39. For a survey of UK cybercrime, see National Cyber Security Centre and National Crime Agency, 'The Cyber Threat to UK Business: 2017-2018 Report', April 2018.
40. Matthew Horne, 'Written Evidence Submitted by the National Crime Agency (PSC0009)', <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/home-office-delivery-of-brexit-policing-and-security-cooperation/written/78338.pdf>, accessed 18 June 2019.
41. Babuta, 'No Deal, No Data?'.
42. 'Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community', Article 8.
43. Robert Wright, 'Europol Head Warns of Security "Impediments" after Brexit', *Financial Times*, 7 March 2018.
44. Europol, 'Operational Agreements', <https://www.europol.europa.eu/partners-agreements/operational-agreements>, accessed 18 June 2019.
45. HM Government, 'Technical Note: Security, Law Enforcement, and Criminal Justice', pp. 2–7, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710802/FINAL_INTERNAL_SECURITY_COMBINED.pdf>, accessed 18 June 2019.
46. Theresa May, 'PM Speech at Munich Security Conference: 17 February 2018', 17 February 2018, <https://www.gov.uk/government/speeches/pm-speech-at-munich-security-conference-17-february-2018>, accessed 18 June 2019.
47. House of Commons Home Affairs Committee, 'UK-EU Security Cooperation after Brexit', Fourth Report of Session 2017–19, HC 635, March 2018, ss. 34–54.

It is hard to find any British or European commentators who relish this prospect. At present, only EU countries are allocated a voting place on the Europol Management Board and a non-EU UK would presumably be therefore excluded. British suggestions for a bespoke arrangement, such as by the House of Commons Home Affairs Committee, propose that the UK retain its place on the board 'with a formal say in the strategic priorities and direction of the agency'.[48] At first blush, it is hard to imagine the EU acceding to this but the committee justifies this proposal because it reflects 'the UK's leadership role in [Europol] since 2009, and its world-leading strength in policing and intelligence'.[49] There is at present no treaty mechanism to allow this to happen and it would require a European Council decision to amend facilitating legislation. The obstacle is therefore not so much legal as political, and it remains to be seen whether this British argument can persuade the Council, especially as not all in the EU accept the claims that the UK is a net security contributor.[50] Without it or something similar, the UK's capacity to tackle cybercrime and many other issues will be diminished over the short-to-medium term. Notably, the EU will be affected similarly.

Outside the Room?

This situation points to one of the more vexing aspects of Brexit. If the UK leaves the EU, particularly if no deal is reached, it will effectively relinquish its capacity to shape EU policy and strategy in multiple fields, including cyber security. Its negotiating leverage as a third country will be limited and its ability to contribute to internal EU defence and security debates will be severely restricted. Diplomacy will continue and the UK will still be a member of other European institutions, like the Council of Europe and the Organization for Security and Co-operation in Europe (OSCE), but it will not be a leading member of the EU as it is now. The House of Lords has noted with concern the implications of being 'outside the room' of security decision-making.[51] In the absence of treaty mechanisms that outline specific arrangements to the contrary, the UK will, as outlined above, de jure be a third-party state to many of the cyber security arrangements in which it presently plays a shaping, if not leading, role. Options are possible that would enable the UK to participate in these institutions, but there is no reason to assume these will be as beneficial to the UK as before Brexit.

This break will occur just when both the EU and the UK are making important steps forward in cyber security. ENISA is in an expansion phase, with a permanent legal mandate probable in 2020, and will play a greater role in cross-EU cyber security coordination and certification, backed by higher levels of funding and resources.[52] The UK is capitalising on increased government investment in cyber security and, through the NCSC and its programme of work, has revised how it interacts with cyber security stakeholders, an approach that seems to be bearing fruit.[53] The UK's Active Cyber Defence programme, for example, is a suite of technical initiatives that brings together public and private entities to tackle cybercrime in the UK and, potentially, elsewhere.[54] The UK and the EU have found new ways of working together, albeit with the UK as a full member state. The incorporation into UK law of the NIS Directive, for instance, is an important regulatory move towards incentivising better cyber security in critical infrastructure systems.[55] This is not to suggest that either body has 'cracked' the cyber security nut – no one has – but each is engaging with cyber security, and with each other, in robust and productive fashion.

Following Brexit, each party will find it that much harder to work with the other, although one should not discount the high levels of trust that pertain in information security and transnational

48. *Ibid*., s. 53.
49. *Ibid*.
50. House of Commons Home Affairs Committee, 'UK-EU Security Cooperation after Brexit: Follow-up Report', Seventh Report of Session 2017–19, HC 1356, ss. 34–35.
51. House of Lords European Union Committee, 'Brexit: The Proposed UK-EU Security Treaty', 18th Report of Session 2017–19, HL Paper 164, s. 69.
52. European Commission, 'EU Negotiators Agree on Strengthening Europe's Cybersecurity', press release, 10 December 2018, <http://europa.eu/rapid/press-release_IP-18-6759_en.htm>, accessed 18 June 2019.
53. National Cyber Security Centre, 'Annual Review 2018', 2018.
54. Tim Stevens et al., 'UK Active Cyber Defence: A Public Good for the Private Sector', Cyber Security Research Group and the Policy Institute, King's College London, January 2019.
55. National Cyber Security Centre, 'NCSC NIS Guidance – Introduction to the NIS Directive', <https://www.ncsc.gov.uk/collection/nis-directive?curPage=/collection/nis-directive/introduction-to-the-nis-directive>, accessed 18 June 2019.

policing communities as a mitigating factor. It will be impossible for the UK to remain a member of the NIS Cooperation Group or the CSIRTs Network without a legal foundation, or to have a formal role in the determination of future changes in EU cyber security or data protection regulation. The UK is compliant with the EU General Data Protection Regulation 2016, but what arrangements will be forthcoming for ensuring compliance, upon which UK–EU trade in services may well depend, should EU regulations change in the future? Lessons will doubtless have to be learned from EU data protection agreements with other third countries, such as the recent 'adequacy' decisions for Japan, Switzerland, the US and others.[56] In these cases, the European Commission has determined that non-EU countries satisfy EU data protection requirements, thereby allowing the transfer of EU personal data to and from those third countries.

However, as senior officials past and present have correctly noted, the UK is not as reliant on the EU for cyber security purposes as some might think. The UK is an important member of NATO, which has its own cyber security objectives, although these are more 'defence'-oriented than those of the EU. It supports the Convention on Cybercrime of the Council of Europe, which is not an EU institution, and will continue to encourage others to sign and ratify the convention, despite its flaws.[57] The UK is involved with cyber security confidence-building measures via the OSCE, which include a range of information-sharing and crisis management initiatives.[58] It was also the initiator of the London Process in 2011, which provides for the international exchange of views between governments, civil society and the private sector.[59] This international role is further underlined by the 2018 Commonwealth Cyber Declaration, announced in London by Prime Minister May, which affirmed the need for international cyber security cooperation across the 53 members of the Commonwealth, particularly in the area of cybercrime.[60] This commitment was bolstered by £15 million of additional funding to Commonwealth partners to carry out cyber security capacity reviews, in addition to the cyber security capacity-building programme already in place at the Foreign Office.[61] The tilt towards the Commonwealth may indicate a quiet shift towards exploring export and influence opportunities afforded by deeper cyber security relationships with Commonwealth countries. This would also serve to bolster the UK's trade portfolio under the 'Global Britain' rubric.[62]

Brexit will not affect in principle the dominant position of the US in both US–UK and US–EU security relations, but it will influence the character of these relationships. The UK's principal security partner will continue to be the US and, whether EU countries like it or not, the US will persist as their key security ally too. In cyber security policy and practice, the US is the global leader, and where the US goes others tend to follow, albeit sometimes reluctantly. Following Brexit, however, might the UK lean away from the EU and further towards the US to shore up a creaking 'special relationship'? Will it be able to continue acting as a bridge between the US and the EU on issues like data protection and cyber resilience? Indeed, will the UK be able to fulfil this role anyway, if it ceases to be, in the minds of both itself and Five Eyes partners (especially the US), a gateway to European partners for cooperation and insight? And – given the purported recent decision by the Cabinet to allow Huawei to participate in the UK's 5G network development, albeit at a low level[63] – how might this both affect its security relationship with a US government vociferously opposed to allowing Chinese telecom giants to participate in the US domestic market, or the UK's need to form renewed relationships with China in a post-Brexit trade construct?

56. European Commission, 'Adequacy Decisions', <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>, accessed 18 June 2019.
57. Council of Europe, 'Details of Treaty No. 185 – Convention on Cybercrime', <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>, accessed 18 June 2019.
58. Organization for Security and Co-operation in Europe, 'OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies', Decision No. 1202, 10 March 2016.
59. William Hague, 'London Conference on Cyberspace: Chair's Statement', speech given in London, 2 November 2011.
60. The Commonwealth, 'Commonwealth Cyber Declaration', made at the Commonwealth Heads of Government Meeting, London, 20 April 2018.
61. Prime Minister's Office, 'UK Commits to a Safer Commonwealth in Cyber Space', press release, 17 April 2018, <https://www.gov.uk/government/news/uk-commits-to-a-safer-commonwealth-in-cyber-space>, accessed 18 June 2019.
62. House of Commons Foreign Affairs Committee, 'Global Britain and the 2018 Commonwealth Summit', Seventh Report of Session 2017–19, HC 831, April 2018.
63. Dan Sabbagh, 'Huawei Dilemma is a Question of Britain's Post-Brexit Future', *The Guardian*, 24 April 2019.

In any of these scenarios, the UK will continue to have good relationships with most EU countries, with shared values and interests, as noted in the Political Declaration of 2018. This situation is challenged by domestic political forces across Europe, including those expressed in Brexit, but there are reasons to be optimistic when thinking about future international cyber security cooperation and coordination, although there will inevitably be some recalibration of priorities and activities. Not least, the UK and the EU will find common cause in countering active cyber threats emanating from states like Russia and China – and those states' cyber diplomacy – and perhaps in mitigating a growing rift between the US and its transatlantic allies.[64]

Conclusion

As with so much else, the contours of the future UK–EU cyber security relationship are contingent on the broader political-strategic context, including the presence of sufficient goodwill on either side as may survive the current state of uncertainty and acrimony. The mutual interest in cooperation and collaboration will be affected by the conduct and outcome of UK–EU negotiations, but too much has already been developed – and too much is at stake – to damage irreparably, let alone abandon, the close working relationships already in place. It is true that many aspects of cyber security cooperation will continue as they did before, but the UK and the EU will have to work harder than ever to maintain the quality of those interactions, while others may vanish without formal frameworks to sustain them. As outlined above, this will be particularly necessary in the fields of information sharing and cybercrime, arrangements for which may require new legal mechanisms subject to the jurisdiction of the ECJ.

Moreover, if the EU and the UK are required to negotiate two security treaties – one on 'internal' police and security matters, the other on 'external' defence and foreign policy cooperation – how will cyber security, which is rooted in both, be dealt with? UK government statements on Brexit say little about the role of cyber security as an object or driver of defence strategy or foreign policy, and hint instead that it would fall under an internal security treaty.[65] This is not unreasonable, but, given the diversity of cyber security issues – from cyber threat intelligence sharing to cyber defence, cyber resilience, and nation-state cyber-enabled information operations – there will need to be greater attention to cyber security in any forthcoming UK–EU treaty negotiations. In the absence of a withdrawal treaty, it is likely that at least one defence and security treaty will be needed, in which cyber security must be addressed by both parties as a strategic priority.

It remains to be seen how Brexit will affect the UK's reputation in defence and security, particularly if a withdrawal agreement cannot be approved by Parliament. In respect of cyber security, for example, will Brexit impact the UK's stated objective to strengthen collective cyber security through deepening 'existing links with our closest international partners'?[66] Britain's international cyber security networks and working relationships will not wither away after Brexit, but it is naive to expect they can remain precisely as they did before the UK's exit from the EU. Perhaps what is needed is for the UK to rediscover and reassert its fabled pragmatism, as a component of what Lord Ricketts has called 'an energetic, active, distinctive British foreign policy'.[67] Cyber security can play its part in promoting this ambition, capitalising on its undoubted strengths in this field while at the same time recognising where it needs to bolster its efforts in respect of its European partners. If, as the industry adage has it, 'cyber security is a team sport', the UK needs to recognise and embrace this as a matter of urgency, rather than inadvertently damage national cyber security obligations and aspirations. ■

Tim Stevens is Senior Lecturer in the Department of War Studies, King's College London.

Kevin O'Brien is Senior Visiting Research Fellow in the Department of War Studies, King's College London.

64. Katie Rogers and David E Sanger, 'Among European Allies, Americans Offer Competing Visions', *New York Times*, 16 February 2019.
65. HM Government, 'Framework for the UK-EU Security Partnership', May 2018, p. 26.
66. HM Government, 'National Cyber Security Strategy 2016-2021', p. 9.
67. House of Lords Select Committee on International Relations, 'UK Foreign Policy in a Shifting World Order', 5th Report of Session 2017-19, HL Paper 250, December 2018, s. 292.